情報処理学会論文誌　コンシューマ・デバイス & システム　Vol.9　No.2　22–32 (May 2019)

コンシューマ・システム論文

環境発電デバイスのサイドチャネル評価システムと耐タンパ実装の開発

野崎 佑典[1,a)]　吉川 雅弥[1]

受付日 2018年10月9日, 採録日 2019年1月31日

概要：環境発電デバイスの利用が期待されており，セキュリティを確保するための暗号化に関する検討も行われている．一方で，暗号回路を対象としたサイドチャネル解析の脅威が報告されており，環境発電デバイスにおける耐タンパ性に関する研究は非常に重要である．本研究では，環境発電デバイスに対するサイドチャネル評価システムを開発し，その耐タンパ性について評価する．また，環境発電デバイスの安全性を向上させるための耐タンパ実装を開発する．そして，実環境発電デバイスを用いた評価実験により，開発したサイドチャネル評価システムと耐タンパ実装の有効性を評価する．

キーワード：環境発電，サイドチャネル解析，耐タンパ性，ハードウェアセキュリティ

Development of Evaluation System for Side-channel Analysis and Tamper Resistant Implementation of Energy Harvester

Yusuke Nozaki[1,a)]　Masaya Yoshikawa[1]

Received: October 9, 2018, Accepted: January 31, 2019

Abstract: Since energy harvesters have attracted attention, investigations for encryption of energy harvesters to ensure the security have been performed. On the other hand, the threat of side-channel analysis for a cryptographic circuit is pointed out. Therefore, it is important to study the tamper resistance for energy harvesters. This study develops the side-channel analysis evaluation system for energy harvesters, and evaluates its tamper resistance. This study also develops a tamper resistant implementation for energy harvesters to improve the tamper resistance. Experiments using an actual energy harvester evaluate the validity of the developed side-channel analysis verification system and the tamper resistant implementation.

Keywords: energy harvesting, side-channel analysis, tamper resistance, hardware security

1. はじめに

近年，コンシューマ製品に Internet of Things（IoT）が導入されており，スマートウォッチ等のウェアラブルデバイスからスマートホーム，ヘルスケア等多岐の分野で実用化がなされている [1]．IoT の導入により，消費者にとってよりよいサービスが提供され，新たなビジネスモデルの構築が期待されている．一方で IoT の普及に関して，電源やセキュリティの課題が指摘されている [2]．

まず電源の課題に関して，IoT 機器の増加に従い，電源配線や電池交換にかかるコストについての問題が指摘されている [2]．そのため，電源の課題を解決するための技術として，環境発電が注目されている [3], [4], [5], [6], [7]．環境発電は，光や振動，電波，熱等のエネルギーを電気エネルギーへと変換する技術である．環境発電を利用することで，電源配線や電池交換を必要としないバッテリレスなシステムが構築できるため，IoT の電源課題の解決が期待されている．

次にセキュリティの課題に関して，IoT 機器では，やり取りされる情報の漏洩を防ぐためのデータの秘匿化や，改ざんやなりすましを防ぐための認証を行うことが重要である [2]．これらのセキュリティ対策の実現には暗号技術の

[1] 名城大学
Meijo University, Nagoya, Aichi 468–8502, Japan
[a)] 143430019@ccalumni.meijo-u.ac.jp

利用が不可欠である．そのため，環境発電デバイスでの暗号化に関する検討も行われている [8]．

ここで暗号アルゴリズムは計算量的にその安全性が保障されているが，暗号処理時に発生する電磁波や電力等の情報を利用した解析（サイドチャネル解析）に対して脆弱であることが指摘されている [9], [10], [11], [12], [13], [14], [15], [16]．サイドチャネル解析では，サイドチャネル情報を利用した統計処理を行うことで，回路内部の秘密鍵を推定する．そのため，デバイスの安全性を確保するうえで，サイドチャネル解析に対する耐性評価（耐タンパ性評価）を行うことは非常に重要である．これまでに，IC カードや FPGA，ASIC 等に実装された暗号回路に対する耐タンパ性評価は数多く報告されている [17] が，環境発電デバイスを対象とした研究は見当たらない[*1]．

そこで本研究では，環境発電デバイスの耐タンパ評価システムを開発する．また，環境発電デバイスでのサイドチャネル解析に対する安全性を向上させるための耐タンパ実装を開発する．そして，実際の環境発電デバイスを使用した評価実験を行い，開発システムと開発耐タンパ実装の有効性について評価する．

2. 準備

まず，2.1 節では本研究で使用する環境発電デバイスについて，2.2 節では環境発電デバイス上に実装する軽量暗号について説明する．そして，2.3 節ではサイドチャネル解析について，2.4 節では関連研究について，2.5 節では本論文の貢献について述べる．

2.1 環境発電デバイス

代表的な環境発電デバイスとして，TWELITE [18] や EnOcean [19] 等がある．TWELITE はモノワイヤレス株式会社によって販売されている環境発電デバイス用マイコンモジュールであり，気象庁の気象・環境観測やスマート農業 [20]，工事現場の保安製品 [21]，介護・見守りシステム [22] 等，国内の様々な分野で採用実績があり，広く用いられている [23]．また，TWELITE と EnOcean の消費電流の比較結果を**表 1** に示す．この比較では，TWELITE と文献 [8] で使用されている EnOcean のデバイス STM400J を比較した．比較には文献 [30] と文献 [31] のデータシートを利用した．表 1 より TWELITE の方がより低消費電力で利用可能なことが分かる．ここで，環境発電デバイスではその発電量は限られており，限られた発電量で暗号化や耐タンパ実装を行うためには，より低消費電力と動作するデバイスが必要だと考えられる．そのため本研究では，環境発電デバイスに TWELITE を使用する．具体的に，TWELITE を搭載した無線通信モジュール TWELITE-DIP と太陽光発電用電源管理ユニット TWE-EH SOLAR，太陽電池（Panasonic AM-5815）を環境発電デバイス（子機）として使用する．親機には，TWELITE を搭載した MONOSTICK を使用し，子機との無線通信を行う．環境発電デバイス（子機）と MONOSTICK（親機）の外観を**図 1** に示す．

[*1] 通常，耐タンパには開封検知という意味も含まれるが，本論文では開封検知の意味は含まない．

表 1　TWELITE と EnOcean の比較
Table 1　Comparison of TWELITE and EnOcean.

	送信電流 [mA]	受信電流 [mA]
TWELITE	15.3	17
EnOcean	23	27

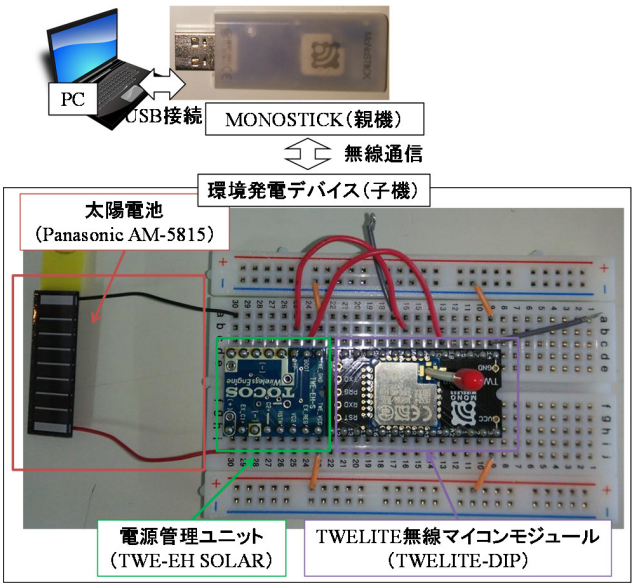

図 1　TWELITE 環境発電デバイス（子機）と MONOSTICK（親機）の外観
Fig. 1　Appearance of TWELITE energy harvester and MONOSTICK.

TWELITE は，32 bit の RISC マイコンを内蔵し，Universal Asynchronous Receiver Transmitter（UART）や Serial Peripheral Interface（SPI），Inter-Integrated Circuit（I2C），Analog to Digital Converter（ADC）等のインタフェースを搭載している．また，無線通信は 2.4 GHz 帯を使用しており，規格は IEEE802.15.4 に準拠している．TWELITE の動作に関して，外部から 2.6 [V]～3.6 [V] の電源を供給することで動作させることができる [18]．

このとき，TWELITE を環境発電により動作させるためには，TWE-EH SOLAR と太陽電池を TWELITE-DIP へと接続する．動作に関して，太陽電池で発電したエネルギーは TWE-EH SOLAR に内蔵されているコンデンサへと充電し，以下の処理を行う．

① 太陽電池で発電したエネルギーを TWE-EH SOLAR に内蔵されているコンデンサ（220 [μF]）へ充電する．
② 内蔵コンデンサの電圧が一定の値（約 2.9 [V]）に達す

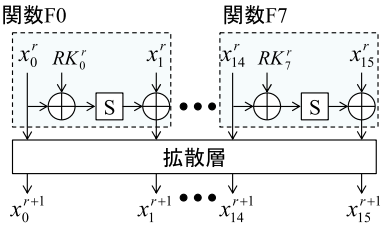

図 2　TWINE のラウンド処理
Fig. 2　Round processing of TWINE.

ると，TWELITE の電源をオンにし，データの無線送信を行う．

③　TWELITE はデータの無線送信のたびにいったんスリープ状態となり，任意のスリープ時間経過後，再び無線送信を行う．

④　内蔵コンデンサの電圧が一定の値（約 2.0 [V]）に下がると，TWELITE の電源をオフにする．

⑤　①から④の動作を繰り返し行う．

2.2　軽量暗号

これまでに，環境発電デバイスでの暗号化に関する研究が報告されており [8]，一般的に広く用いられている AES 暗号と比較して，消費エネルギーの観点から軽量暗号の優位性が示されている．そこで本研究では，代表的な軽量暗号である TWINE [24] を環境発電デバイスに実装する．TWINE はソフトウェア実装において，回路規模・処理速度に関して良好な性能を持つ [24]．TWINE は 16 分割一般化 Feistel 構造のブロック暗号であり，ブロック長は 64 bit，鍵長は 80 bit と 128 bit の 2 種類から選択できる．本研究では 80 bit の秘密鍵を用いる．そして，暗号化では 64 bit の平文に対し，36 回のラウンド処理を行うことで，64 bit の暗号文を生成する．

TWINE のラウンド処理の詳細を**図 2** に示す．図 2 に示すように，ラウンド処理は 8 つの関数 F（関数 F0 から関数 F7）と拡散層（転置処理）で構成する．各関数 F は S-BOX による非線形な置換処理と，ラウンド鍵 RK や暗号中間値 x との XOR 演算で構成する．具体的に，r ラウンド目の処理を式 (1) に示す．

$$\begin{cases} x^{r+1}_{h(2j)} = x^r_{2j} \\ x^{r+1}_{h(2j+1)} = S(x^r_{2j} \oplus RK^r_j) \oplus x^r_{2j+1} \end{cases} \tag{1}$$

ただし，$S(\ )$ は S-BOX の処理，$h(\ )$ は拡散層の処理，$\oplus$ は XOR 演算，$j = 0, 1, \ldots, 7$ である．

TWINE は 1 ラウンド目から 35 ラウンド目までは，式 (1) の処理を行い，最終ラウンドである 36 ラウンド目では，拡散層を除いた処理を行う．したがって，暗号文 c は式 (2) で計算される．

$$\begin{cases} c_{2j} = x^{36}_{2j} \\ c_{2j+1} = S(x^{36}_{2j} \oplus RK^{36}_j) \oplus x^{36}_{2j+1} \end{cases} \tag{2}$$

2.3　サイドチャネル解析

サイドチャネル解析は，サイドチャネル情報を利用した統計処理により，暗号回路内部の秘密鍵を推定する [14]．特に漏洩電磁波を利用した解析は電磁波解析と呼ばれ，代表的な解析手法として相関電磁波解析（Correlation ElectroMagnetic Analysis：CEMA [16]）が知られている．

CEMA では，暗号中間値のハミング重みやレジスタ間のデータのハミング距離とその時に生じる電磁波との相関関係を解析に利用する．ハミング重みを利用した解析では，暗号処理の S-BOX 等の非線形処理の出力の遷移確率の偏りに着目する．具体的には，既知の暗号文と鍵の候補値を利用した計算により S-BOX の出力値を予測し，出力値のハミング重み H と電磁波 W とのピアソンの相関係数 ρ を式 (3) より計算する．

$$\rho_t = \frac{\sum_{i=1}^{N}(W_{i,t} - \overline{W_t})(H_i - \overline{H})}{\sum_{i=1}^{N}(W_{i,t} - \overline{W_t})^2 \sum_{i=1}^{N}(H_i - \overline{H})^2} \tag{3}$$

ただし，$\overline{W_t}$ は電磁波 W の平均，$\overline{H}$ はハミング重み H の平均，N は解析に使用する波形の数，t は波形データの時間軸上のサンプル点である．そして，相関係数を最大とする鍵の候補値を正解鍵として推定する．

2.4　関連研究

これまでに，環境発電のセキュリティに関する研究として，環境発電デバイスの暗号化についての研究が報告されている [8]．文献 [8] は，利用可能な消費エネルギーの観点から環境発電デバイスにソフトウェア実装可能な暗号技術について検討している．具体的には，EnOcean を対象に，AES 暗号と軽量暗号 SPECK を実装し，EnOcean のセキュリティプロトコル使用時の消費エネルギーについて比較している．その結果，ブロック長と鍵長が最小構成の SPECK（ブロック長：32 bit，鍵長：64 bit）は暗号化が可能であり，AES 暗号と比較して消費エネルギーの観点から，軽量暗号が優位であることを示している．

また，ハードウェアレベルで環境発電技術を耐タンパ実装に応用する研究も行われている．文献 [25] では，環境発電における電源管理技術を利用することで，主電源と暗号回路動作の電源を分離させる．攻撃者は，回路全体（主電源）の消費電力しか観測できないため，電力解析やタイミング解析に対する耐性を向上させることができる．しかし文献 [25] では，RTL や SPICE を用いたシミュレーションによる検証のみが行われており，実デバイスを用いた評価は行われていない．

耐タンパ性評価に関する研究としては，暗号回路の安全性を評価するために統一的な環境を構築することを目的とした SASEBO（Side-channel Attack Standard Evaluation

BOard）プロジェクトが知られている [17]．SASEBO プロジェクトでは，Xilinx 社の FPGA に対応した SASEBO-G や SASEBO-GII，Altera 社の FPGA に対応した SASEBO-B，ASIC の暗号 LSI を搭載した SASEBO-R，IC カードに対応した SASEBO-W 等が開発されている．しかし，これまでに環境発電デバイスの耐タンパ性評価に関する研究は筆者らの知る限り報告されていない．

2.5　本論文の貢献

本論文の貢献は以下のとおりである．

- 新たに環境発電デバイスの耐タンパ評価システムを開発し，環境発電デバイスの耐タンパ性を定量的に評価した．
- 環境発電デバイスに実装する軽量暗号 TWINE のソフトウェア実装における，耐タンパ性評価手法を提案した．
- 環境発電デバイス向けの処理時間の増加を抑えた耐タンパ実装を新たに開発し，その有効性を定量的に評価した．

3.　開発耐タンパ評価システム

3.1　システムの概要

本研究で開発する耐タンパ評価システムについて説明する．開発システムの概略図を**図 3** に示す．図 3 に示すように開発システムは，暗号処理を行う TWELITE 環境発電デバイス（子機），子機の暗号化データを受信する親機（MONOSTICK），太陽光発電用 LED ライト，オシロスコープ等の測定系で構成する．このとき MONOSTICK で受信したデータは TeraTerm を用いてログデータとして保存する．また，TWELITE の開発環境には TWELITE NET SDK を使用した．TWELITE NET SDK はモノワイヤレス株式会社から無償で提供されているソフトウェア開発環境であり，統合開発環境 Eclipse 上で C 言語を用いた開発が可能である．そして，Web [18] 上に無償で公開されている，親機と子機で無線通信を行う無線タグアプリ（App_Tag [26]）をベースに開発を行った．開発では，暗号アルゴリズムとして軽量暗号 TWINE をソフトウェア実装した．プログラムの書き込みに関して，書き込みライタには TWELITE R-トワイライターを，書き込みソフトには TWELITE プログラマを使用した．プログラムの書き込みの様子を**図 4** に示す．

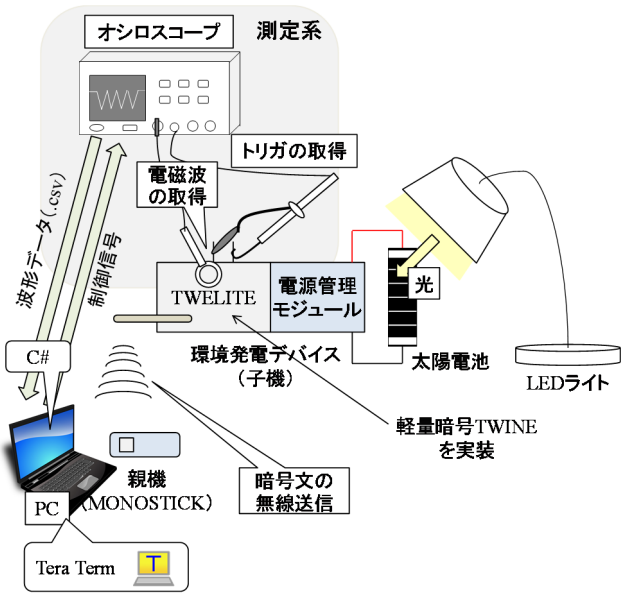

図 3　開発耐タンパ評価システムの概要

Fig. 3　Outline of the developed tamper resistance evaluation system.

ここで，耐タンパ性評価では，サイドチャネル情報（波形データ）の測定において，波形データの時間軸上での同期をとるために，トリガ信号を取得する必要がある [14]．そこで，開発システムでは TWINE 暗号処理時にデバイス外部にトリガ信号を出力できるようプログラムを変更した．具体的には，**図 5** に示すように暗号化（図の Cipher）の前後に，TWELITE の DO3 ピンを Hi にする記述（vPortSetHi）を追加した．

また波形取得に関して，SASEBO 等の評価環境では，安定した電源により評価ボードは動作し，評価ボードとオシロスコープ等の測定器を PC から制御することで，必要なデータを自動測定している [17]．具体的に，波形取得時には，PC からオシロスコープへ波形取得命令を送信する．その後，評価ボードに暗号化命令を送信し，暗号化を行い，このときのサイドチャネル情報をオシロスコープで取得す

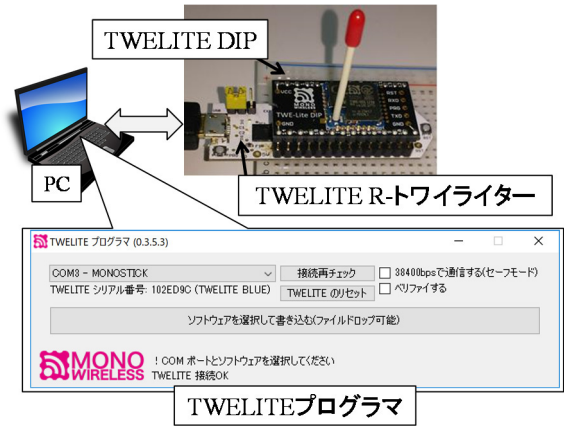

図 4　プログラムの書き込みの様子

Fig. 4　Writing of program.

```
255    //Trigger ON
256    vPortSetHi(PORT_OUT3);
257
258    Cipher(data,RoundKey);//Encryption processing
259
260    //Triger OFF
261    vPortSetLo(PORT_OUT3);
```

図 5　トリガ信号のための記述

Fig. 5　Description for trigger signal.

Algorithm 1: Acquire waveform

```
Acquire ( ) /* Acquire waveform */
/* Check the status of oscilloscope */
status_reg ← Read_status ( )
while status_reg = true do
    status_reg ← Read_status ( )
end while
```

る．一方で，環境発電デバイスは環境発電による不安定な電源で動作しており，どのタイミングでデバイスが動作するかを把握することは難しい．また開発システムでは，環境発電デバイスは無線通信によりデータをやりとりしているため，PC から直接暗号化のタイミングを制御することはできない．そこで開発システムでは，波形取得のために，オシロスコープに波形取得命令を送信後，環境発電デバイスの暗号化終了時まで，待機する処理を行う．具体的には，オシロスコープ内部の状態レジスタを監視し，波形を取得するまで待機する．疑似コードを Algorithm 1 に示す．

次に，耐タンパ性評価では暗号文と波形データは同期している必要があり，この同期がとれない場合，耐タンパ性評価を行うことは難しい [14]．しかし，予備実験において TWELITE 環境発電デバイスでは，暗号化実施時に暗号処理は行われるが，暗号文の送信失敗，もしくは親機のデータ受信の失敗が確認された．このとき，トリガ信号は出力されるため，オシロスコープ側で波形の取得処理は行われるが，暗号文の取得処理は行われない．したがって，**図 6** に示すように暗号文と波形データの同期ずれが発生する．図 6 の例では，$X+1$ 回目の暗号化の際，$X+1$ 個目の波形データは取得されるが，データの送受信の失敗により暗号文は取得されない．そして，次の $X+2$ 回目の暗号化では，$X+2$ 個目の波形データと $X+1$ 個目の暗号文が取得され，取得した波形データの数と暗号文の数の差，すなわち同期ずれが発生している．そこで開発システムでは，同期ずれを解決するために，**図 7** に示すように子機に内部カウンタを導入する．内部カウンタは暗号処理ごとに値を 1 つずつ増加させる．そして，暗号文と内部カウンタを親機へと無線送信する．図 7 の例では，図 6 の例と同様に，同期ずれが発生しているが，取得した暗号文の数である $X+1$ と内部カウンタ値である $X+2$ を参照することにより，値のずれから同期ずれを検出することができる．以上のように，開発システムでは，図 7 に示すように親機で取得した内部カウンタの値を参照することで，実際に取得した波形データと暗号文の同期ずれが発生しているかどうかを確認することができる．最後に，TeraTerm で取得できるログデータの例を**図 8** に示す．図 8 に示すように暗号文や内部カウンタの値を参照することができる．また，図 8 の例では取得した暗号文の数は 1,001 で，内部カウンタは 1,007 であり，2 つの値には差があり，同期ずれが検出できていることが確認できる．

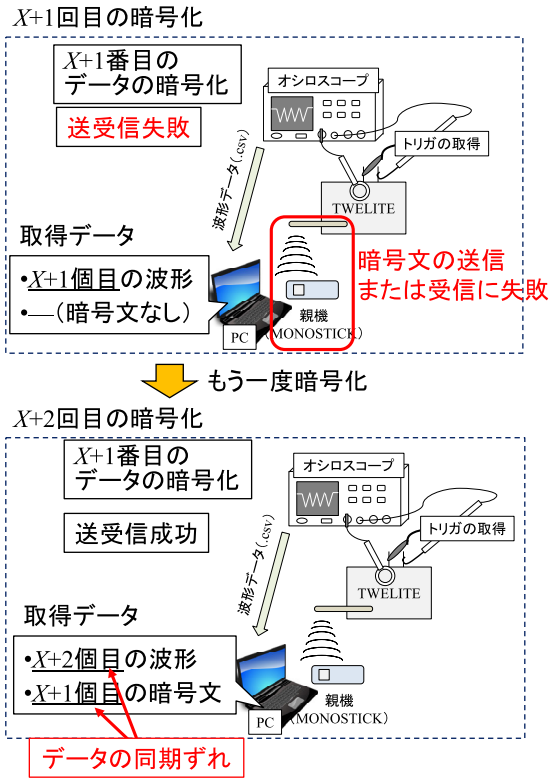

図 6　暗号文と波形の同期ずれ

Fig. 6　Synchronization deviation between ciphertext and waveform.

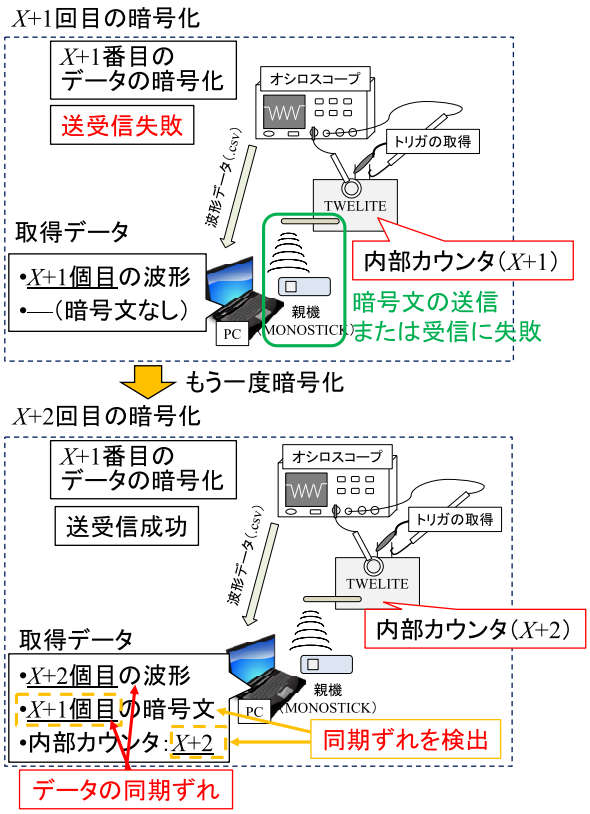

図 7　同期ずれの検出

Fig. 7　Detection of synchronization deviation.

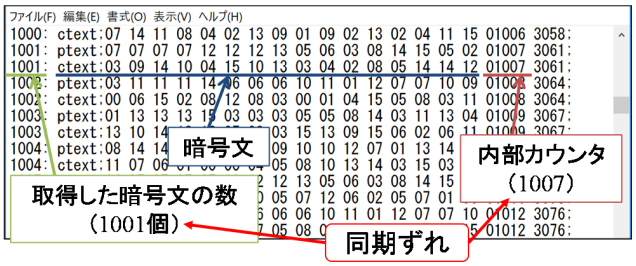

図 8　TeraTerm のログデータの例
Fig. 8　Example of log data in TeraTerm.

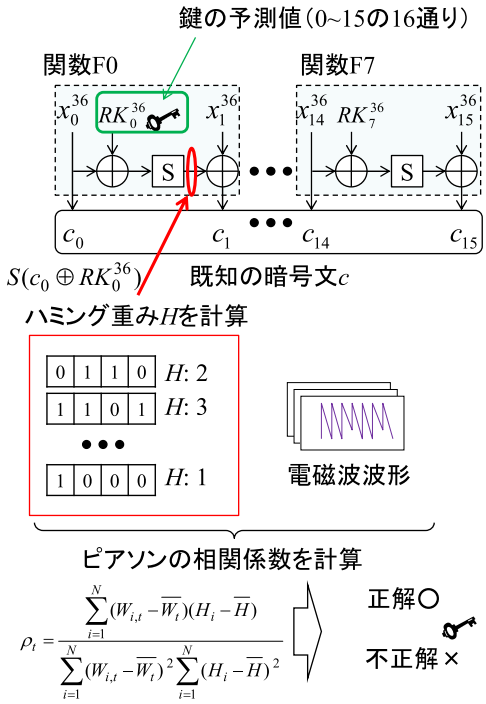

図 9　TWINE に対する電磁波解析
Fig. 9　Electromagnetic analysis for TWINE.

3.2　評価手法

耐タンパ性評価は，3.1 節で説明した環境で取得した暗号文と波形を利用して，TWINE に対して CEMA を適用することで行う．ここで，TWINE に対する耐タンパ性評価手法に関して，ハードウェア実装を対象としたものは提案されている [27] が，ソフトウェア実装を対象としたものは報告されていない．

そこで本研究では，ソフトウェア実装した TWINE の耐タンパ性評価手法を提案する．ここで，サイドチャネル解析では非線形処理の計算値に着目することで解析を行う [14]．また，TWINE では S-BOX で非線形処理が行われているため，S-BOX を解析の対象とする．提案する耐タンパ性評価手法では，解析に暗号文を用いるため，**図 9** に示すように TWINE の 36 ラウンド目の S-BOX の出力値のハミング重み H を解析に用いるものとする．このとき，ハミング重み H は式 (4) で計算できる．

$$H = HW(S(c_{2j} \oplus RK_j^{36})) \tag{4}$$

ただし，$HW(\,)$ はハミング重み H を求める関数である．このとき，暗号文 c は既知であるが，ラウンド鍵 RK_j^{36} は未知である．そのため，ラウンド鍵 RK_j^{36} には予測値を用いる．このとき，式 (4) のラウンド鍵 RK_j^{36} は 4 bit の値であるため，予測値には 0 から 15 までの 16 通りの値をすべて試行する．そして，求めたハミング重みと電磁波との相関係数を式 (3) より計算し，正解鍵を推定する．

4.　開発耐タンパ実装

本研究で開発する耐タンパ実装について説明する．開発耐タンパ実装では，比較的容易に実現可能なアルゴリズムレベルでの対策を施す．ここで，環境発電デバイスは，環境発電により得られる微小な電力により動作するため，耐タンパ実装では低消費電力で実現可能な対策が求められる．一般的に，ソフトウェア実装における消費電力はマイコンの命令実行サイクル，すなわち処理時間に依存することが知られている [8]．

耐タンパ実装に関して，代表的なものにマスキングとハイディングが知られている [11], [12], [13], [14]．マスキングは乱数を用いた XOR 演算（マスク処理）を行うことで，秘密情報との相関を隠ぺいする対策である [11]．具体的に，各演算の前後にマスク処理とアンマスク処理（マスクを外す XOR 演算）を適用する．このとき，S-BOX 等の非線形な演算では，マスクされた値の非線形処理後の値にアンマスク処理を適用した場合，通常の S-BOX 計算結果と異なる値となる．そのため，マスク処理では整合性を満たすために，あらかじめマスクされた計算結果に合わせた S-BOX を複数個用意する．そのため，事前に多くの計算が必要であり，回路規模や処理時間が増加する [11], [12], [13]．

ハイディングには，ダミー演算対策とシャッフリング等の手法が知られている [11]．ダミー演算対策は，通常の演算とは異なるダミー演算をランダムに挿入することで，暗号処理時の消費電力を時間軸方向でランダム化する [11]．また，挿入するダミー演算の数を増やすほど，耐タンパ性を向上させることができる．しかし，ダミー演算対策は新たに演算を挿入するため，ダミー演算の数だけ処理時間が増加する [11]．次に，シャッフリングは各演算の実行順をランダムに入れ替えることで，時間軸方向で消費電力をランダム化させる [11], [14]．シャッフリングは演算を入れ替えるのみであるため，新たに追加する処理は少なく，処理時間の増加を抑えることができる．

本研究では，最も処理時間の増加が少ないと考えられるシャッフリングを用いた耐タンパ実装を開発する．開発耐タンパ実装では，TWINE の各 S-BOX 処理に対応する関数 F（関数 F0 から F7）に対してシャッフリングを適用する．開発耐タンパ実装の概要を**図 10** に示す．図 10 の①は無対策の場合の例（通常の実行順）を，図 10 の②はシャッフリングを適用した場合の例をそれぞれ示している．図 10

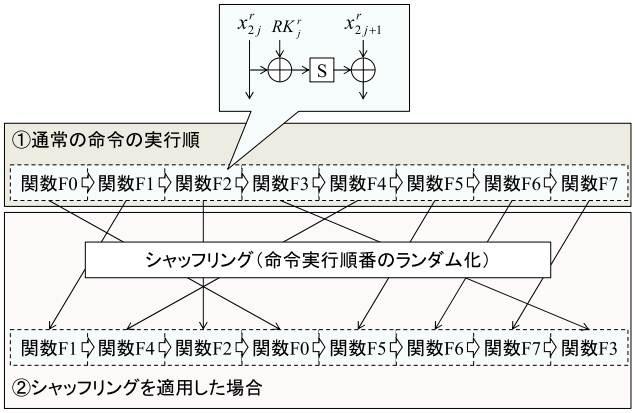

図 10　開発耐タンパ実装
Fig. 10　Developed tamper resistant implementation.

Algorithm 2: Developed tamper resistant implementation

Input: x, RK
　　$rand$ /* random number */
for $0 \leq j \leq 7$ do
　/* LFSR $(x^3 + x^2 + 1)$ */
　$shift \leftarrow (rand \ \& \ 0x01) \oplus ((rand \ \& \ 0x02) \gg 1)$
　$rand \leftarrow (rand \gg 1) \mid (shift \ll 2)$
　$k \leftarrow rand$
　/* F function with shuffling */
　$x_{2k+1} \leftarrow S\,(x_{2k} \oplus RK^i_k) \oplus x_{2k+1}$
end for

の②に示すように，シャッフリングにより各関数 F の実行順をランダムに変化させることができる．

また，各ラウンド処理のシャッフリングに使用する乱数には，3 bit の乱数値をシード値とした線形帰還シフトレジスタ（Linear Feedback Shift Register：LFSR）を使用した．この LFSR には，周期が 7 となる帰還多項式 $x^3 + x^2 + 1$ を使用し，LFSR の出力値に対応した関数 F を実行することでランダム化を実現させる．疑似コードを Algorithm 2 に示す．

5.　評価実験

開発システムの有効性を評価するために評価実験を行った．まず 5.1 節では，実験環境について述べる．そして，5.2 節では無対策のデバイスを用いた実験とその評価について，5.3 節では対策済みのデバイスを用いた実験とその評価について述べる．

5.1　実験環境

まず無対策の環境発電デバイスに対して耐タンパ性評価を行い，開発システムの有効性について検証した．実験環境を**図 11** と**表 2** に示す．実験では，攻撃者の立場で様々な条件下での解析を想定し，環境発電の有無，すなわち電源が安定している場合と不安定な場合での耐タンパ性評価へ与える影響を検証するために，TWELITE を環境発電

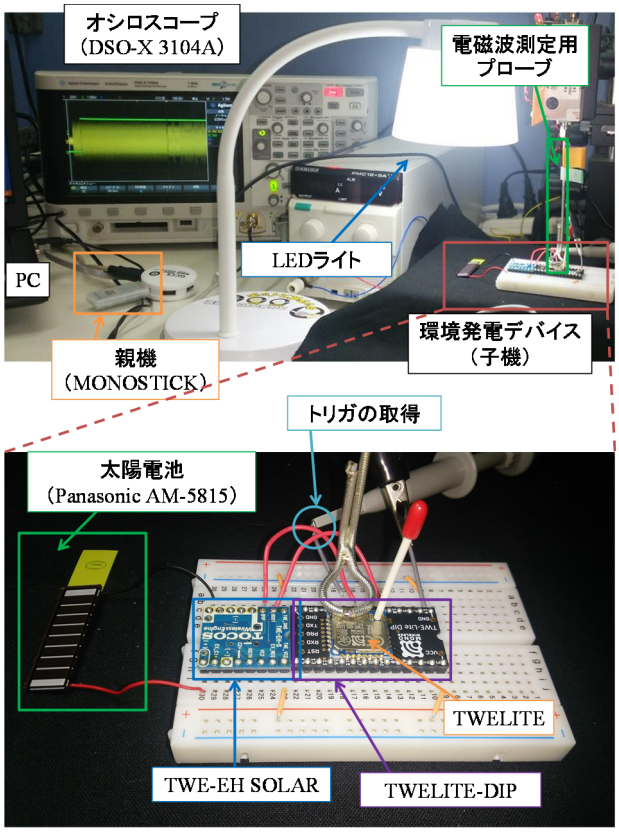

図 11　開発システム
Fig. 11　Development system.

表 2　実験環境の詳細
Table 2　Detail of experimental condition.

TWELITE 環境発電デバイス	Panasonic AM-5815 TWE-EH SOLAR TWELITE-DIP
親機	MONOSTICK
LED ライト	DS-LS06-W
暗号アルゴリズム	TWINE
平文	ランダムに生成
オシロスコープ	Agilent DSO-X 3104A
サンプリングレート	5 [Gsa/sec]
電磁波測定用アンテナ	シールディッドループアンテナ
電磁波測定用 RF アンプ	MITEQ AU-3A-0150

（太陽電池）で動作させた場合と，安定化電源で動作させた場合でそれぞれ行った．環境発電を用いる場合では，安定して光を照射させるために，LED ライトを太陽電池の直上で固定した．ここで，実験で使用した LED ライトは照度を 100%，50%，20%の 3 段階で変化させることができる．また，直下約 25 cm のものに対して，100%で光を照射させた場合，その照度は約 1,000 [lx] 以上となる．さらに実験では，照度の違いによる耐タンパ性評価への影響を検証するために，照度を 100%にした場合と 50%にした場合の 2 段階で変化させて行った．一方で，安定化電源を

用いる場合では，3.3 [V] の電圧を供給して実験を行った．電磁波の測定には，シールディッドループアンテナとオシロスコープを使用した．アンテナの配置の拡大図を**図 12** に示す．アンテナの配置に関して，TWELITE の上部が最も測定した電磁波の強度が大きくなったため，上側で固定した．アンテナの向き・距離に関して，向きは TWELITE に対してアンテナのループ開口面が水平になるように固定し，距離は TWELITE に対してアンテナが接触しない範囲で最も近い距離で固定した．そして，1,000 種類のランダム平文の暗号化時の電磁波を測定した．

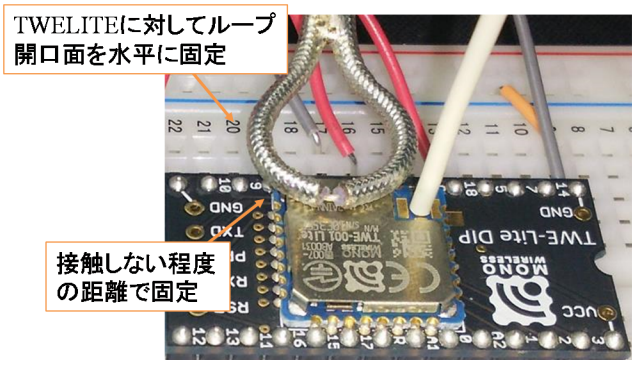

図 12　シールディッドループアンテナの拡大図
Fig. 12　Enlarged view of shielded loop antenna.

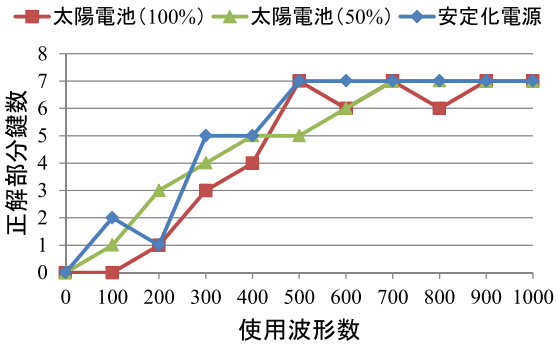

図 13　耐タンパ性評価結果（無対策）
Fig. 13　Result of the tamper resistance evaluation without the tamper resistant implementation.

5.2　無対策のデバイスを用いた実験とその評価

開発システムを用いて，環境発電デバイスの耐タンパ性を評価した．実験結果を**図 13** に示す．図 13 の縦軸は解析に成功した部分鍵の数を，横軸は評価に使用した電磁波波形の数を示している．図 13 に示すように，環境発電で動作させた（太陽電池を使用した）場合と安定化電源を使用した場合のどちらの場合においても，900 個の電磁波波形を使用することで，8 個中 7 個の部分鍵の解析に成功していることが分かる．ここで，残り 1 つの部分鍵が解析できていないのは，電磁波解析による局所性が原因の 1 つだと考えられる．具体的に，電磁波解析には局所性があり，プローブの位置や向き，角度によりその解析効率が変わることが知られている [28], [29]．また，環境発電を用いた場合に関して，照度が 100%と 50%のどちらにおいても，900 波形で 7 個の部分鍵の解析に成功している．ここで，TWELITE 環境発電デバイスでは太陽電池で持続的に光エネルギーを取り入れ，内蔵コンデンサへの充電を行っている．そのため，環境発電の微小な発電量であっても，安定して暗号処理が可能であり，開発システムにより耐タンパ性評価が可能であると考えられる．

次に，鍵候補別の解析結果を**図 14** に示す．図 14 は各部分鍵における鍵候補別の相関係数を示したものである．各グラフの赤い丸で囲ってある部分はそれぞれ正解鍵での結果を示している．図 14 より，8 番目の部分鍵（不正解だった部分鍵）以外は，正解鍵で最も相関係数が大きくなっていることが確認できる．

また，正解鍵での相関係数の結果を**図 15** に示す．図 15 は 36 ラウンド目処理時の相関係数であり，横軸は時間を示している．図 15 よりそれぞれ，相関係数のピークが表れていることが確認できる．このとき，部分鍵によってピークの表れる位置（時間軸）が異なっている．これは TWINE

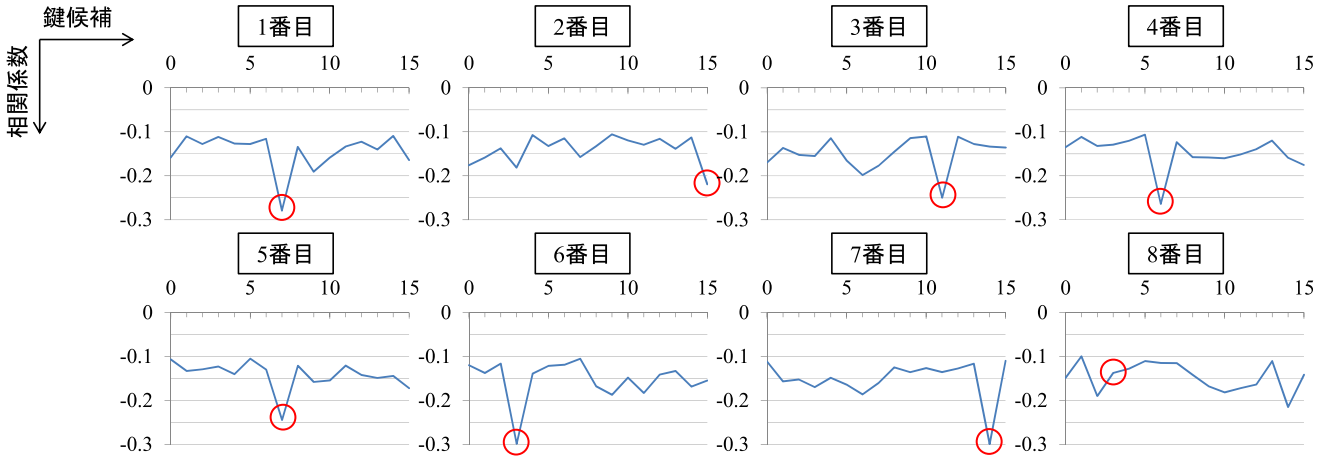

図 14　鍵候補別の解析結果
Fig. 14　Results for each key candidate.

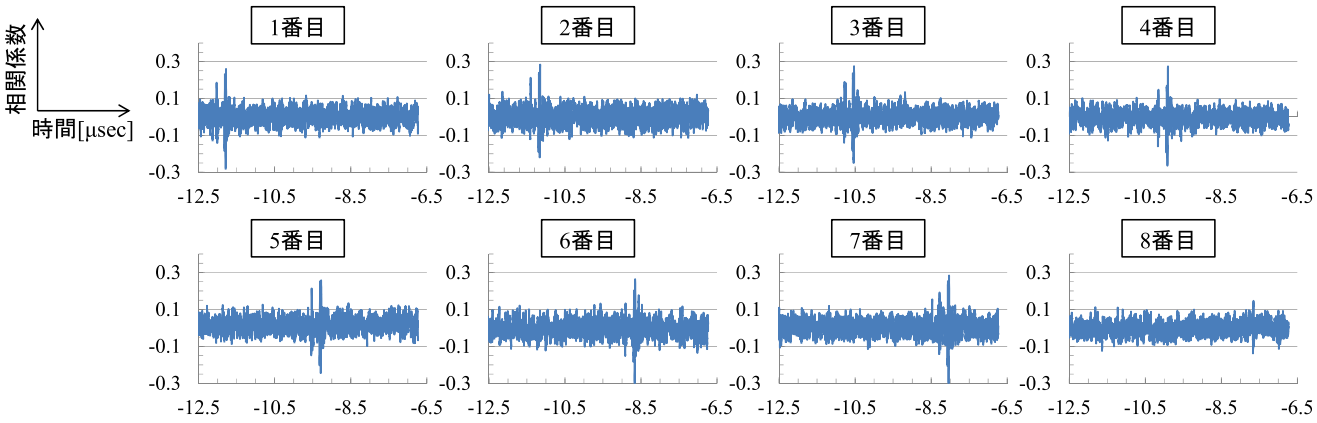

図 15　各正解鍵における相関係数

Fig. 15　Correlation coefficient for each correct partial key.

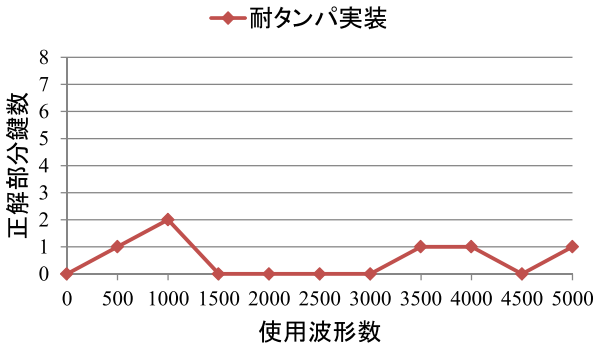

図 16　耐タンパ性評価結果（開発耐タンパ実装）

Fig. 16　Result of the tamper resistance evaluation with the developed tamper resistant implementation.

表 3　実行時間の比較

Table 3　Comparison of execution time.

	時間[μsec]
無対策	623
開発耐タンパ実装	782

のソフトウェアの暗号処理では，各命令が逐次的に実行されているからだと考えられる．

5.3　対策済みのデバイスを用いた実験とその評価

次に，開発耐タンパ実装の有効性について評価した．この実験では，環境発電デバイスに開発耐タンパ実装を施した．そして，100%の照度の光による環境発電によりデバイスを動作させた．またこの実験では，5,000 個の電磁波波形を使用した評価を行った．実験結果を**図 16** に示す．図 16 に示すように，5,000 個の電磁波波形を用いた場合でも，正解した部分鍵の数は 1 つであることが確認できる．したがって，開発耐タンパ実装により，時間軸方向でのランダム化が行われ，耐タンパ性が向上していると考えられる．

また，環境発電デバイスの消費電力に関わる実行時間について比較した．比較結果を**表 3** に示す．表 3 に示すように，開発耐タンパ実装は無対策と比較して，実行時間は増加しており，その増加は 1.25 倍程度であることが確認できる．これは，シャッフリングのために乱数生成を行っていることが原因だと考えられる．

6.　まとめ

本研究では，今後コンシューマ製品での利用が期待される環境発電デバイスの耐タンパ評価システムを開発した．そして，実デバイスを用いた評価実験により開発システムにより耐タンパ性評価ができることを実証した．また，環境発電デバイスのサイドチャネル解析に対する安全性を向上させるための耐タンパ実装を開発した．開発耐タンパ実装では，最も実行時間の増加が少ないと考えられるシャッフリングを適用することで，時間軸方向での処理のランダム化を図り，耐タンパ性を向上させた．そして，開発システムを用いた評価により，開発耐タンパ実装の有効性を確認した．

今後は，開発システムを振動発電等の他の環境発電デバイスへ適用する予定である．また，ダミー演算対策等の他の耐タンパ実装に関しても，その性能について検討を進める予定である．

謝辞　本研究の一部は，JSPS 科研費 17J11408 の助成を受けたものです．

参考文献

[1] Alioto, M. and Shahghasemi, M.: The Internet of Things on Its Edge: Trends Toward Its Tipping Point, *IEEE Consumer Electronics Magazine*, Vol.7, No.1, pp.77–87 (2018).

[2] Sicaria, S., Rizzardia, A., Griecob, L.A. and Coen-Porisinia, A.: Security, privacy and trust in Internet of Things: The road ahead, *Computer Networks*, Vol.76, pp.146–164 (2015).

[3] Chalasani, S. and Conrad, J.M.: A Survey of Energy Harvesting Sources for Embedded Systems, *Proc. IEEE SoutheastCon 2008*, pp.442–447 (2008).

[4] Tentzeris, M.M., Georgiadis, A. and Roselli, L.: Energy

Harvesting and Scavenging, *Proc. IEEE*, Vol.102, No.11, pp.1644–1648 (2014).
[5] 竹内敬治：エネルギーハーベスティング技術，電気評論，Vol.97, No.11, pp.51–55 (2012).
[6] 堀越　智，竹内敬治，篠原真毅：エネルギーハーベスティング　身の周りの微小エネルギーから電気を創る “環境発電”，日刊工業新聞社 (2014).
[7] Nicosia, A., Pau, D., Giacalone, D., Plebani, E., Bosco, A. and Iacchetti, A.: Efficient Light Harvesting for Accurate Neural Classification of Human Activities, *Proc. IEEE Int. Conf. Consumer Electronics* (*ICCE 2018*), pp.1–4 (2018).
[8] 坂本純一，松本　勉：環境発電無線センサモジュールにソフトウェア実装可能な共通鍵暗号，2016 年暗号と情報セキュリティシンポジウム講演論文集，2C4-1, pp.1–8 (2016).
[9] Kocher, P., Jaffe, J. and Jun, B.: Differential Power Analysis, *Proc. CRYPTO '99*, LNCS 1666, pp.388–397, Springer-Verlag (1999).
[10] Brier, E., Clavier, C. and Olivier, F.: Correlation Power Analysis with a Leakage Model, *Proc. 6th Int. Workshop Cryptographic Hardware and Embedded Systems* (*CHES 2004*), LNCS 3156, pp.16–29, Springer-Verlag (2004).
[11] Messerges, T.S.: Securing the AES Finalists Against Power Analysis Attacks, *Proc. Int. Workshop on Fast Software Encryption* (*FSE 2000*), LNCS 1978, pp.150–164, Springer (2000).
[12] Akkar, M.-L. and Giraud, C.: An Implementation of DES and AES, Secure against Some Attacks, *Proc. 2nd Int. Workshop Cryptographic Hardware and Embedded Systems* (*CHES 2001*), LNCS 2162, pp.309–318, Springer-Verlag (2001).
[13] Herbst, C., Oswald, E. and Mangard, S.: An AES Smart Card Implementation Resistant to Power Analysis Attacks, *Proc. Int. Conf. Applied Cryptography and Network Security* (*ACNS 2006*), LNCS 3989, pp.239–252, Springer (2006).
[14] Mangard, S., Oswald, E. and Popp, T.: Power Analysis Attacks, p.338, Springer (2007).
[15] Gandolfi, K., Mourtel, C. and Olivier, F.: Electromagnetic Analysis: Concrete Results, *Proc. 3rd Int. Workshop on Cryptographic Hardware and Embedded Systems* (*CHES 2001*), LNCS 2162, pp.251–261, Springer-Verlag (2001).
[16] Meynard, O., Guilley, S., Danger, J.-L. and Sauvage, L.: Far Correlation-based EMA with a Precharacterized Leakage Model, *Proc. Design, Automation and Test in Europe Conference and Exhibition* (*DATE 2010*), pp.977–980 (2010).
[17] 片下敏宏，佐藤　証：暗号ハードウェアの実装性能と物理的安全性評価，電子情報通信学会論文誌 A，Vol.J95-A, No.5, pp.392–406 (2012).
[18] モノワイヤレス株式会社，入手先 ⟨https://mono-wireless.com/jp/index.html⟩.
[19] EnOcean, available from ⟨https://www.enocean.com/⟩.
[20] Suzaki, T., Minematsu, K., Morioka, S. and Kobayashi, E.: TWINE: A Lightweight, Versatile Blockcipher, *Proc. ECRYPT Workshop on Lightweight Cryptography* (*LC11*), pp.146–149 (2011).
[21] スマートロジック株式会社製品概要，入手先 ⟨http://www.smartlogic.jp/⟩.
[22] NEXCO 中日本製品ラインナップ，入手先 ⟨http://products.c-nexco-hmn.jp/#item33⟩.
[23] 株式会社ベイビッグ製品情報，入手先 ⟨http://www.baybig.co.jp/html/product.html⟩.
[24] モノワイヤレス株式会社採用事例，入手先 ⟨https://mono-wireless.com/jp/casestudies/index.html⟩.
[25] Moukarzel, M. and Hicks, M.: Reap What You Store: Side-channel Resilient Computing Through Energy Harvesting, *Proc. 5th ACM Int. Workshop on Energy Harvesting and Energy-Neutral Sensing Systems* (*ENSsys '17*), pp.21–26 (2017).
[26] モノワイヤレス株式会社無線タグアプリ（App_Tag），入手先 ⟨https://mono-wireless.com/jp/products/TWE-APPS/App_Tag/index.html⟩.
[27] 野崎佑典，藤野　毅，吉川雅弥：軽量暗号 TWINE に対する周波数領域での電力解析とその評価，電子情報通信学会論文誌 B，Vol.J99-B, No.10, pp.881–892 (2016).
[28] 庄司陽彦，角尾幸保，板倉征男：FPGA に対する漏洩電磁波の局所性を利用した電磁波解析，2010 年暗号と情報セキュリティシンポジウム講演論文集，3B3-2, pp.1–6 (2010).
[29] 森田秀一，松本　勉，高橋芳夫，四方順司：暗号ハードウェアの局所情報と電磁波解析（その 3），2011 年暗号と情報セキュリティシンポジウム講演論文集，2D3-2, pp.1–7 (2011).
[30] TWELITE 無線マイコンデータシート，入手先 ⟨https://mono-wireless.com/jp/products/TWE-LITE/MW-PDS-TWELITE-JP.pdf⟩.
[31] Scavenger Transceiver Module STM 400J DATA SHEET, available from ⟨https://www.enocean.com/jp/enocean-modules-928mhz/details/stm-400j/data-sheet-pdf⟩.

野崎 佑典　（学生会員）

2016 年 3 月名城大学大学院理工学研究科情報工学専攻修士課程修了．同年 4 月，同大学大学院理工学研究科電気電子・情報・材料工学専攻博士後期課程入学，現在に至る．2014～2015 年 CREST プロジェクトに参加．暗号 LSI のセキュリティに関する研究に従事．電子情報通信学会回路とシステム研究会学生優秀賞，IEEE GCCE2015 Excellent Poser Award，情報処理学会第 19 回 CDS 研究発表会学生奨励賞等受賞．電子情報通信学会，IEEE の各会員．

吉川 雅弥　（正会員）

2001 年 3 月立命館大学大学院理工学研究科博士課程修了．博士（工学）．同大学理工学部第 1 号助手・講師を経て，2007 年 4 月名城大学理工学部准教授，2012 年 4 月より教授．2009〜2015 年 CREST 研究員．LSI 設計・設計自動化技術の研究に従事．第 3 回 LSI IP デザインアワード開発奨励賞，第 10 回 LSI IP デザインアワード研究助成賞，FIT2003 ベストペーパー賞，2007 年度システム制御情報学会産業技術賞，CAINE2010 Best Paper Award，WCECS2011 Best Paper Award 等受賞．電気学会，電子情報通信学会，システム制御情報学会，日本知能情報ファジィ学会，IEEE の各会員．